AD-A050 745 GEORGIA INST OF TECH ATLANTA SCHOOL OF INFORMATION A--ETC F/G 9/2
A PROBABILISTIC REMARK ON ALGEBRAIC PROGRAM TESTING.(U)
MAY 77 R A DEMILLO, R J LIPTON DAAG29-76-G-0338
UNCLASSIFIED GIT-ICS-77/07 ARO-14690.3-M NL

| OF |

AD
A050745

END
DATE
FILMED
4 -78
DDC

Unclassified

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

ARO 14690.3-M

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER 18 ARO
19 14690.3-M

2. GOVT ACCESSION NO.

3. RECIPIENT'S CATALOG NUMBER

4. TITLE (and Subtitle)
6 A Probabilistic Remark on Algebraic Program Testing.

5. TYPE OF REPORT & PERIOD COVERED
9 Technical ~~Report~~,

6. PERFORMING ORG. REPORT NUMBER
14 GIT-ICS-77/07

7. AUTHOR(s)
10 Richard A. DeMillo
Richard J. Lipton

8. CONTRACT OR GRANT NUMBER(s)
15 DAAG29-76-G-0338

9. PERFORMING ORGANIZATION NAME AND ADDRESS
School of Information and Computer Science
Georgia Institute of Technology
Atlanta, Georgia 30332

10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS

11. CONTROLLING OFFICE NAME AND ADDRESS
U. S. Army Research Office
Post Office Box 12211
Research Triangle Park, NC 27709

12. REPORT DATE
11 May 77

13. NUMBER OF PAGES
5 12 9p.

14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office)

15. SECURITY CLASS. (of this report)
Unclassified

15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

The findings in this report are not to be construed as an official Department of the Army position, unless so designated by other authorized documents.

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Program Testing
Multinomials
Algebra
Probability
Computer programs
Computer systems programs

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

A key step in Howden's method (Howden, W. E., "Algebraic Program Testing" ~~Computer Science Technical~~ Report No. 14, November 1976, UC-San Diego, La Jolla, CA.) for algebraic program testing requires checking the algebraic identity of multinomials. Howden's solution requires evaluations in at least 2^m points for m-ary multinomials. This note presents a probabilistic solution which achieves small probability of error on 30 points.

2 to the mth power

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

JOB

Unclassified

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

410 044

ACCESSION for

NTIS	White Section	X
DDC	Buff Section	☐
UNANNOUNCED		☐
JUSTIFICATION		
BY		
DISTRIBUTION/AVAILABILITY CODES		
Dist.	AVAIL. and/or SPECIAL	
A		

GIT-ICS - 77/07

(Technical Report)

A PROBABILISTIC REMARK ON ALGEBRAIC PROGRAM TESTING

Richard A. DeMillo
School of Information and Computer Science
Georgia Institute of Technology
Atlanta, GA 30332

Richard J. Lipton
Computer Science Department
Yale University
New Haven, CT 06520

MAY 1977

TECHNICAL REPORT

School of Information and Computer Science
Georgia Institute of Technology
Atlanta, GA 30332

ABSTRACT: A key step in Howden's method [5] for algebraic program testing requires checking the algebraic identity of multinomials. Howden's solution requires evaluations in at least 2^m points for m-ary multinomials. This note presents a probabilistic solution which achieves small probability of error on 30 points.

Until very recently, research in software reliability has divided quite neatly into two -- usually warring -- camps: methodologies with a mathematical basis and methodologies without such a basis. In the former view, "reliability" is identified with "correctness" and the principle tool has been formal and informal verification [1]. In the latter view, "reliability" is taken to mean the ability to meet overall functional goals to within some predefined limits [2,3]. We have argued in [4] that the latter view holds a great deal of promise for further development at both the practical and analytical levels. Howden [5] proposes a first step in this direction by describing a method for "testing" a certain restricted class of programs whose behavior can -- in a sense Howden makes precise -- be *algebraicized*. In this way, "testing" a program is reduced to an equivalence test, the major components of which become

(i) a combinatorial identification of "equivalent" structures;

(ii) an algebraic test

$$f_1 \equiv f_2 ,$$

where f_i, $i = 1, 2$ is a multivariable polynomial (multinomial) of degree specified by the program being considered.

In arriving at a method for exact solution of (ii), Howden derives an algorithm which requires evaluation of multinomials $f(x_1, \ldots , x_m)$ of maximal degree d at $O(d + 1)^m$ points. For large values of m (a typical case for realistic examples), this method becomes prohibitively expensive.

Since, however, a test for reliability rather than a certification of correctness is desired, a natural question is whether or not Howden's method can be improved by settling for less than an exact solution to (ii).

We are inspired by Rabin [6] and, less directly, by the many successes of Erdös and Spencer [7] to attempt a *probabilistic* solution to (ii). Using these methods, we show that (ii) can be tested with probability of error ε with only $O(g(\varepsilon))$ evaluations of multinomials, where g is a slowly growing function of only ε. In particular, 30 or so evaluations should give sufficiently small probability of error for most practical situations. The remainder of this note is devoted to proving this result.

Let us denote by $P_{\not\equiv 0}(m,d)$ the class of multinomials

$$f(x_1, \ldots, x_m) \not\equiv 0$$

(over some arbitrary but fixed integral domain) whose degree does not exceed $d > 0$. We define

$$P(m,d,r) = \min_{f \,\in\, P_{\not\equiv 0}(m,d)} \text{Prob}\,\{1 \leq \underset{\sim}{x}_1 \leq r,\ f(\underset{\sim}{x}_1, \ldots, \underset{\sim}{x}_m) \not\equiv 0\}$$

We think of $P(m,d,r)$ as the minimal relative frequency with which witnesses to the non-nullity of a multinomial of the appropriate kind can occur in the choosen interval. Notice, in particular, that since a polynomial of degree d has at most d roots (ignoring multiplicity), the largest probability of finding a root must be at least the probability of finding a root by randomly sampling in the interval $1 \leq \underset{\sim}{x}_1 \leq r$; thus

$$P(1,d,r) \geq 1 - d/r\ .$$

Now, consider some

$$f(x_1, \ldots, x_m, y) \not\equiv 0$$

of degree at most d. But there are then multinomials $\{g_i\}_{i \leq d}$, not all $\not\equiv 0$, such that

$$f(x_1, \ldots, x_m, y) = \sum_{i=0}^{d} g_i(x_1, \ldots, x_m) y^i .$$

Let us suppose that $g_k \in P_{\neq 0}(m,d)$. Thus

$$\text{Prob}\,\{1 \leq \underset{\sim}{x}_i \leq r,\ f(\underset{\sim}{x}_1, \ldots, \underset{\sim}{x}_m, y) \neq 0\}$$

$$\geq \text{Prob}\,\{g_k(\underset{\sim}{x}_1, \ldots, \underset{\sim}{x}_m) \neq 0 \text{ and } y \text{ is not a root}\}$$

$$\geq P(m,d,r)(1 - d/r) .$$

Continuing inductively, we obtain

$$P(m,d,r) \geq (1 - d/r)^m \tag{1}$$

But

$$\lim_{m \to \infty} (1 - d/r)^m = \lim_{m \to \infty} \left[1 + \frac{1}{m}\left(\frac{-dm}{r}\right)\right]^m = e^{\frac{-dm}{r}} . \tag{2}$$

Combining (1) and (2), we have for large m, r = dm,

$$P(m,d,dm) \geq e^{-1} .$$

Thus, with t evaluations of f for independent choices of points from the m-cube with sides r = dm, the probability of missing a witness to the non-nullity of $f(x_1, \ldots, x_m)$ is at most

$$(1 - e^{-1})^t .$$

Table 1 shows the probable error in testing $f \equiv 0$ by t evaluations of f at randomly chosen points for some typical values of d,m,r,t.

		$[1 - P(m,d,r)]^t$				
dm	r	t=10	t=20	t=30	t=50	t=100
10	10	1.0×10^{-2}	1.0×10^{-3}	1.0×10^{-6}	1.1×10^{-10}	1.2×10^{-20}
20	10	0.23	5.5×10^{-2}	1.3×10^{-2}	7.0×10^{-4}	4.8×10^{-7}
50	10	0.93	0.87	0.82	0.71	0.51
10^2	10	1.0	1.0	1.0	1.0	1.0
10	10^2	6.0×10^{-9}	$<10^{-20}$	$<10^{-20}$	$<10^{-20}$	$<10^{-20}$
20	10^2	3.9×10^{-8}	1.5×10^{-15}	$<10^{-20}$	$<10^{-20}$	$<10^{-20}$
50	10^2	8.9×10^{-5}	7.9×10^{-9}	7.0×10^{-13}	$<10^{-20}$	$<10^{-20}$
10^3	10^2	1.0	1.0	1.0	1.0	1.0
10	10^3	$<10^{-20}$	$<10^{-20}$	$<10^{-20}$	$<10^{-20}$	$<10^{-20}$
20	10^3	9.3×10^{-18}	$<10^{-20}$	$<10^{-20}$	$<10^{-20}$	$<10^{-20}$
50	10^3	7.6×10^{-14}	$<10^{-20}$	$<10^{-20}$	$<10^{-20}$	$<10^{-20}$

Table 1. Probable Error in Testing $f(x_1, \ldots, x_m) \equiv 0$
(degree $\leq$ d) by t random evaluations in $\{1, \ldots, r\}$

Notice that for dm = r, t = 30, this is already $< 10^{-5}$.

References

1. Manna, Z., *Mathematical Theory of Computation*, McGraw-Hill, 1974.

2. Brown, J. R., Lipow, M., "Testing for Software Reliability," *Intern. Conf. in Reliable Software*, SIGPLAN Notices, 10, 6, (June 1975), pp. 518-527.

3. Llewelyn, A. I., Wilkins, R. F., "The Testing of Computer Software," *1969 Conf. on Software Engineering*, pp. 189-199.

4. DeMillo, R. A., Lipton, R. J., Perlis, A. J. "Social Processes and Proofs of Theorems and Programs," *Fourth ACM Symposium in Principles of Programming Languages*.

5. Howden, W. E., "Algebraic Program Testing" Computer Science Technical Report No. 14, November 1976, UC-San Diego, La Jolla, CA.

6. Rabin, M. O., "Probabilistic Algorithms," in J. Traub, editor, *Algorithms and Complexity*, Academic Press, 1976, pp. 21-40.

7. Erdös, P., Spencer, J., *Probabilistic Methods in Combinatorics*, Academic Press, 1974.